**FEDERAL TRADE COMMISSION**
**Washington, D.C. 20580**

# COMMENTS OF THE NATIONAL RETAIL FEDERATION

## Federal Identity Theft Task Force,

**FTC Project No. P065410**


**Mallory B. Duncan**
*Senior Vice President*
*General Counsel*

**Elizabeth T. Oesterle**
*Senior Director*
*Government Relations Counsel*

The National Retail Federation
325 7th Street, N.W.
Suite 1100
Washington, D.C. 20004
(202) 783–7971


January 19, 2007

**Federal Identity Theft Task Force**
**Comments of the National Retail Federation**

On behalf of the members of the National Retail Federation we respectfully submit the following comments. By way of background, the **National Retail Federation** is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail establishments, more than 24 million employees - about one in five American workers - and 2006 sales of $4.7 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations.

For criminals, identity theft is a crime with relatively low risks and, often, high rewards. According to a 2003 report, identity thieves face only a 1 in 700 chance of being caught[1]. Although ID theft has commonly been called "a 21st century crime," most identity crimes are committed using relatively unsophisticated means. Reports highlight information stolen in pre-existing relationships, familial I.D. theft, pick-pockets taking wallets or purses, and mail interception as common causes of the crime.[2] Statistics published by Bureau of Justice Statistics ("BJS") in April, 2006, also seem to further suggest that I.D. crimes are well-targeted. According to BJS, households most likely to experience ID theft, broadly defined, earned $75,000 or more, are between the ages of 18-24, or live in urban or suburban areas.[3] Because most ID thieves seem to use "old-fashioned" techniques and to target their victims, it is important to also point out that relatively few ID thefts have been attributed to "sophisticated" data breaches despite the perception that the consumers whose information may have been jeopardized are at great risk of being victimized.

As a result of the string of highly publicized "data breach" disclosures in 2005 and 2006, including the Choice Point, Bank of America, Card Systems and Veterans' Affairs Administration incidents, members of Congress and the Executive Branch are taking a hard look at the way personally identifiable information ("PII") is secured and the kinds of steps that should be taken in the event that information is compromised. The President's Identity Theft Task Force ("Task Force") was given the important role of looking at the federal government's use of PII, developing a coordinated strategic plan to combat identity theft and to make recommendations on ways to further improve the effectiveness and efficiency of the federal government's efforts to combat ID theft. The Task Force's initial findings released on September 19, 2006, were introspective to the

[1] "Identity Theft, 2004, First Estimates form the National Crime Victimization Survey," Bureau of Justice Statistics, April 2006.
[2] "Identity Theft Soars, Remains Lower Tech Crime," *TechWeb.com*, July 21, 2003.
[3] Bureau of Justice Statistics, April 2006.

federal government and raised many important questions about the storage and management of sensitive information. The draft "Strategic Plan" that surfaced just a few weeks later was quite different from the President's original mandate and, while it did call for changes within the federal government regarding law enforcement initiatives, the use and display of social security numbers ("SSNs") and the creation of data breach guidelines, its focus seemed to dramatically shift to the private sector.

## National Data Security Standards

There is currently no federal law that governs all uses of consumer information. The most notable federal financial privacy statute is Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA") that prohibits financial institutions from sharing non-public personally identifiable customer information with non-affiliated third parties without giving consumers an opportunity to opt-out. The act also requires financial institutions (as defined in GLBA) to safeguard the security and confidentiality of customer information. Further, the Fair Credit Reporting Act ("FCRA") governs the way that information may be collected, and by whom it can be used, for "eligibility" purposes, including the granting of credit and conducting employment background checks

The FTC's Financial Information Safeguards Rule ("Safeguards Rule") as required under GLBA took effect in May of 2003. The Safeguards Rule requires financial institutions to develop a written information security program that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. On page 31 of the draft "Strategic Plan," the Task Force asserts that there are "gaps" in the types of businesses subject to the GLBA safeguards and specifies "retail merchants" as an example of uncovered entities. The Task Force further states that, "There is no logical reason why a financial institution holding a consumer's credit card information, for example, should be held to different safeguards standard that a retail merchant holding the exact same information." (Draft "Strategic Plan," p 31). We are pleased that the Task Force has stepped back from this assertion and asked for additional information on this issue. On page 4 of the Request for Public Comment ("RFP") the Task Force asks, "Does the need for such a national standard, if any, vary according to economic sector, business model, or business size?" The answer is a resounding "yes."

Financial institutions, as defined under GLBA, hold much more sensitive information about a customer than just a credit card number – they hold all of the information needed to complete the opening of an account and for conducting a continuing relationship with that customer. The ongoing relationship may include the granting of credit, the offering of financial products, and the periodic checking of the customer's credit report. Further, financial institutions retain sensitive information to comply with a host of state and federal laws and regulations. With that type of relationship comes a well-established fiduciary duty to protect, to the extent possible, sensitive financial information. Most retailers however, only hold a credit card or account number for the purposes of completing a one-off transaction in which

merchandise is given in consideration for payment by the customer (unless that retailer is also offering credit services and is defined as a "financial institutions" as under GLBA). Additionally, the credit card information used or retained by a retailer generally is not sufficient to create new accounts. Instead, the worst type of fraud that can happen, while regrettable, is existing account fraud – a crime with robust consumer remedies as provided under the Truth in Lending Act ("TILA") and the Electronic Funds Transfer Act ("EFTA"). Further, the card associations have established procedures to hold the culpable party responsible for such a breach.

It has become apparent in recent months that the Commission is a pursuing a much broader enforcement strategy when it concerns the safekeeping of consumer information. The B.J.'s consent decree made it clear that the FTC is prepared to take action under Section 5 of the FTC Act when it concludes that any company – not just a financial institution - fails to provide *reasonable and appropriate* security for financial information, even if that company has made no express promises to consumers regarding the privacy or security of sensitive customer information.

If the Task Force is eager to close any perceived "gaps" in current data protection safeguards, why not simply require businesses to establish and implement "reasonable and appropriate," personal information protection policies and procedures? This seems to be the direction that the Commission is already headed. If any additional requirements are needed, the Commission could suggest general guidelines for businesses. It is important to emphasize, however, that no legislative or regulatory regime should go beyond the current FTC Safeguards Rule as applied to financial institutions, and should consider compliance with the current rule as the ultimate "safe harbor" for any business handling sensitive information. Having legislation or regulations that state one or more of these alternatives would give businesses of different types and size much-needed flexibility. This flexibility is also important given the fact that the Commission is a law enforcement agency and not a regulator. If the GLBA Safeguards Rule were adopted across the board, retailers would be at a distinct disadvantage to financial institutions that are regularly subject to examination by bank regulators and often aided in their compliance efforts. The Federal Trade Commission, as a law enforcement agency, is unable to provide this type of routine assistance.

<u>An Additional Contextual Suggestion with Regards to a National Data Security Standard</u>

In the B.J's consent decree the Commission specifically notes the fact that the retailer was storing credit card information in violation of "bank rules," and uses non-compliance with these rules as one of several reasons for taking action under Section 5. Further, the draft "Strategic Plan" makes direct mention of the Payment Card Industry (PCI) data security rules (a.k.a. "bank rules") on page 29, citing low retail industry compliance with that program. However, the draft "Strategic Plan" does not fairly reflect the state of play in the PCI context. It leaves the very distinct impression that large

numbers of retailers, and others who handle credit card numbers, are unconcerned about the consequences of losing sensitive data, and, even in the face of stiff fines, are regularly failing to secure account numbers. Without context, this is quite a mischaracterization of the current problem, and in the face of potential enforcement actions by the Commission based on "reasonable and appropriate" security standards, we would be remiss if we did not discuss the compliance problems associated with PCI.

PCI was a hurried re-write of Visa's Internet-focused CISP rules. CISP was launched when the card associations realized that their credit card systems were not sufficiently secure to deal with increasingly sophisticated threats. Sometime after requiring that businesses meet these expanded "CISP" requirements, Visa came to understand that the Internet model did not work in the brick and mortar world, and thus began a series of redo's that led to PCI and continue to this day.

Consequently, PCI has left businesses faced with the prospect of repeatedly modifying their programs to meet less-than-clear card association requirements. New rules have generally been announced with relatively short compliance deadlines through acquiring banks, who themselves have been unable to agree on such simple matters as who is covered and what the coverage requires. Not so incidentally, Visa itself has had problems complying with the requirements it has imposed on others.

As a result, NRF urges the Task Force and the Commission not to consider technical non-compliance with PCI as prima facie evidence of not having implemented "reasonable and appropriate" security measures because few, if any, retailers know how to fully comply with PCI. Furthermore, PCI is a ***private regulatory scheme***, and its objectives should therefore be expected to differ from a public law addressing the same activities. Both the Commission and the Task Force have broader responsibilities, some of which would not be met if PCI were accepted as a de facto or de jure standard of "good security." We respectfully suggest that the drafters should take the time to further investigate the PCI program and that the Commission should examine its reliance on the terms of the PCI program in future enforcement actions.

**Breach Notification Standards for Private Sector Entities Handling Sensitive Consumer Information**

The National Retail Federation has taken the position that a uniform national breach notification law is a worthwhile legislative objective given the proliferation of such laws in the states. However, our members have cautioned against supporting any legislation that does not differentiate between ID theft and credit card fraud, creates a regime that could lead to the over-notification of consumers who are not in real danger of being victimized, includes paper breaches, contains private rights of action and does not adequately preempt existing state laws.

Paper Breaches

The extension of data breach notification laws to paper is an area of particular concern in the retail sector (and should be for all sectors in light of the volumes of paper records they are required to keep in the day-to-day operation of business). While it is conceivable that someone might steal hundreds of thousands or even millions of paper identity records, experience and common sense dictate that this not nearly as likely as in a computer breach where massive losses can happen at the click of a mouse. Tellingly, of the 34 states that have considered and adopted data breach statutes, only two, North Carolina and Hawaii, have specifically included paper.

We urge the Task Force to examine the problems paper coverage presents when considering the cost/benefit consequences of various types of breaches. For example, does the fact that a job seeker's government employment application filled with PII is found to be "missing" from a director's office raise a "significant risk of identity theft"? Does it matter that a contract cleaning crew was in the office the evening before? Should the job applicant be advised of the possible breach? Should such scenarios be repeated millions of times a month?

Further, because of the nature of paper records, versus their electronic cousins, it is often hard to determine if paper documents have been breached and which records have actually been compromised. Would a business actually know if a dishonest employee has broken into the office after hours and photocopied dozens of his colleagues' tax forms? Would any company be able to tell with any certainty which information about its customers was compromised if a box of documents simply vanished? These complications only scratch the surface. If they are to do anything in this area, we strongly recommend that the Commission and the Task Force consider guidelines for securing sensitive paper documents, rather than simply lumping paper in to a "data breach" notification regime.

Definition of Identity Theft

One issue that NRF has consistently highlighted in the ongoing debate on ID theft and data breach legislation is the fundamental difference between identity theft and credit card fraud. Identity crimes can be broken down into two distinct categories: (1) unauthorized use of an existing account or credit card; and (2) identity fraud/theft – a far more pernicious crime. The 2004 BJS statistics published in April of 2006 tease out these distinctions and show that the vast majority of identity crimes fall under the "unauthorized use" category (close to 2.6 million) versus approximately 500,000 true incidents of identity fraud/theft.[4]

As a practical matter, the most sensitive piece of customer information that a retailer possesses is a credit card number. Retailers typically do not have other sensitive information such as SSNs unless they are also a financial institution. Further, a data

[4] Bureau of Justice Statistics, April 2006.

breach resulting in the loss of a credit card number may at worst lead to credit card fraud, which is easily detected and resolved, and not the more insidious crime of identity theft. As a result, the Task Force should treat the breach of credit card account information differently than the breach of more sensitive PII (as in H.R. 3375 as passed by the House Financial Services Committee in the 109th Congress).

It has been suggested that in writing the "Strategic Plan" the drafters were required to use the definition of identity theft contained in the FACT Act or similar statute. However, Congress has provided other parameters to distinguish between the two crimes as they are covered in two *separate* statutes in the criminal code. Identity fraud is found at 18 USC 1028, while access device or credit card fraud is covered by 18 USC 1029.

The FACTA definition of identity theft was also promulgated in the context of a study, not as a final word as to the contours of the problem. Congress clearly could not have meant to prejudge subsequent efforts to address the problem by preventing the Task Force from speaking to the differences between identity theft and credit card / account fraud. Unfortunately, by not maintaining that clear differentiation in the draft "Strategic Plan" (see, e.g. pages 5, 3-4, 19, and discussion of misuse of existing accounts on 15), it conflates and confuses the harms caused by identity theft, which often entails a complicated and time-consuming resolution process, with those caused by existing account fraud for which the protections are much more streamlined under the Truth in Lending Act (TILA) and the Electronic Funds Transfer Act (EFTA).

The criminal code definition of "identity fraud" is much more focused on the problem to which the report is addressed. Given a choice between two conflicting statutory definitions, there is no reason that the two agencies cannot decide to adopt the one most closely tracking the most pernicious problem, for which there is has not been an easy or uniform solution. As the 2004 BJS Study also shows, consumers spend an average of one day resolving account problems, while victims of true ID theft are much more likely have to spend three or more months restoring their good name.[5]

As was discussed, this report is to be delivered to the President, rather than to Congress. Many executive branch agencies, whether it is the VA, the IRS, the Social Security Administration, or others, maintain vast amounts of truly sensitive identity information. Their reliance on and use of credit card information, by contrast, is relatively incidental. There is no reason that the Commission and the Justice Department cannot address this issue in terms most relevant to the parties they are supposed to be addressing. This would not preclude discussion of account fraud, but would relegate it to position more in keeping with its relative importance. In addition, a detailed discussion of PCI would be even less relevant to the primary focus of the report. As was discussed above, PCI is narrowly tailored, in terms of its scope, to *credit card* information.

[5] Id.

Over-notification of consumers

The consequences of the over-notification of consumers in a data breach situations is a very important component of this discussion. It is important to carefully consider what type or degree of a breach event will require notification. NRF has consistently taken the position that only breaches that pose a "significant risk" of identity theft or fraud should be subject to a notification regime. The rationale behind this is simple: as we have seen in the case of GLBA privacy statements, an over-saturation of notices can lead to inaction by consumers.

As a *New York Times* article from 2006 makes clear, not all thefts are the same, "criminals who are after computer hardware … are unlikely to exploit the personal information that happens to be stored inside. But the thefts that carry more risk, security experts say, involve criminals whose target is personal information."[6] The stolen laptop from the Veterans' Affairs Administration underscores the importance of determining when consumers are truly at risk. In that case, the laptop was stolen for its own value, not the value of the information contained in the laptop. The argument can be made that millions of veterans should not have been told of the "breach" until the authorities had enough information to make a valid determination about the motives of the thieves. Was any material harm done in making the VA "breach" public? Probably not; but the incremental effect of putting consumers on high alert over and over again may lead them to ignore future notices when a truly significant event does in fact occur.

## Conclusion

In July of 2003, California became the first state to mandate notification for consumers whose unencrypted personal information was compromised in a data breach situation. The public notices required under that statute created a rash of publicity around data breaches, ID theft and privacy generally, and led to a flurry of legislative activity in this area. Since 2003, thirty-four states and the District of Columbia have assed data breach legislation.

Several bills were introduced in the House and Senate during the 109th Congress dealing with data security, information privacy, and breach notification. No less than six pieces of legislation received committee action (three in the Senate Judiciary Committee alone) and we expect hearings to resume in the 110th Congress.

Proposals being considered by Congress include broad grants of authority to the FTC to create information safeguard rules that would extend to *every* business that maintains PII. All of bills include mandatory breach notification provisions similar to the California law. Most of the proposed legislation also contains mitigation provisions, including credit file monitoring services to help data breach victims guard against identity theft. Finally, three bills called for complete credit report file freezes – a remedy that some members of Congress believe would further protect victims of identity theft. None of these proposals have been adopted.

[6] "Surging Losses, but Few Victims in Data Breaches," *The New York Times*, September 27, 2006.

FACTA provided consumers with new and powerful tools to combat identity theft. Among these were free annual credit reports, placing "red flags" or "fraud flags" on credit reports, and trade-line blocking for identity theft victims. Additionally, Congress mandated that businesses take better care of information about their customers, including requiring credit card number truncation on receipts and devising new rules for the sharing of information among affiliates.

We are concerned that the remedies and protections afforded to consumers under FACTA – a piece of legislation that still has not been fully implemented – have been pushed to the sidelines in the rush to further protect consumers from being victimized by identity crimes. On page 6 of the RFP, the task force suggests gathering information of the effectiveness of existing victim recovery measures under FACTA and current state file freeze laws as part of their ongoing project. NRF would welcome this type of assessment, as it is vital for formulating a national strategy for combating identity theft. A fuller assessment of the role of the government in handling the information it holds or produces about citizens is also clearly warranted.

As the old adage goes, "you don't know where you are going unless you know where you've been." Congress has already done much work in this area, and perhaps the best path forward involves assessing existing tools before *any* new ones have been suggested. We would further implore the Task Force to look at the thirty-four state data breach statutes, and do an analysis on the risks to consumers of over-notification in the event of data breaches. As we have seen in the context of GLBA privacy notices, the best way to create inaction by consumers may be to desensitize them to important issues through over-notification. This is an outcome we should earnestly try to avoid when someone's financial future may truly be at risk.

Respectfully submitted,

Mallory Duncan

Elizabeth Oesterle